

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA,
Plaintiff,
v.
MIKLOS DANIEL BRODY,
Defendant.

Case No. [3:22-cr-00168-WHO-1](#)

**ORDER ON MOTION TO COMPEL
DISCOVERY**

Re: Dkt. No. 51

In this Computer Fraud and Abuse Act prosecution, defendant Miklos Daniel Brody moves to compel discovery of various categories of records from the government. The motion is DENIED. Generally, based on the government’s written and oral assurances that it has disclosed all responsive records in its possession or does not possess any responsive records, there is no further record that I could compel it to produce. Of course, if the government learns of other records that it is obligated to disclose, it must do so. And if it fails to timely disclose records that it possesses and was obligated to disclose, it will not be able to rely on them at trial.

BACKGROUND

I discuss here only those allegations relevant to resolving this motion. The government filed the criminal complaint in this case in March 2021 and an indictment in April 2022. *See* Criminal Complaint (“Compl.”) [Dkt. No. 1]; Indictment [Dkt. No. 40]. Brody worked at First Republic Bank (“FRB”) as a cloud engineer in San Francisco, California. Compl. ¶ 10. The government alleges that, on March 10, 2020, Brody was brought in for a meeting with FRB executives who stated (based, the government claims, on an internal analysis) that Brody had “plugged multiple flash drives into [an FRB] PC laptop and initiated various file transfers” including alleged pornography. *Id.* ¶¶ 11–12. Brody was fired the next day and left the office

1 around 4:30 pm. *Id.* ¶ 13.

2 The government claims that, later that evening, Brody accessed FRB’s computer network,
3 using the laptop to get through its security. *Id.* ¶ 14. He allegedly used his own account name and
4 also “impersonat[ed]” a colleague. *Id.* ¶ 15. Once he was in the system, says the government, he
5 “caused significant damage” by running scripts that deleted code and damaged software. *Id.* ¶ 18.
6 FRB estimated the damage at more than \$220,000. *Id.* ¶ 20. FRB is cooperating with the
7 government. There are several alleged events that occurred after Brody allegedly accessed the
8 FRB network (such as allegedly suspicious behavior by him), but they are not relevant to the
9 present motion.

10 DISCUSSION

11 Brody moves to compel thirteen types of discovery from the government. *See generally*
12 Motion to Compel Discovery (“Mot.”) [Dkt. No. 51]. He brings the motion under both the
13 constitutional requirements set out in *Brady v. Maryland*, 373 U.S. 83 (1963) and *Giglio v. United*
14 *States*, 405 U.S. 150 (1972), and under Federal Rule of Criminal Procedure (“FRCrP”) 16. *See id.*

15 The Supreme Court held in *Brady* and *Giglio* that the government has a constitutional
16 obligation to disclose to the defendant evidence that is exculpatory or impeaching. *See Strickler v.*
17 *Greene*, 527 U.S. 263, 281–82 (1999). Prosecutors must turn over evidence in the government’s
18 possession, custody, or control and have “a duty to learn of any favorable evidence known to the
19 others acting on the government’s behalf in the case.” *Kyles v. Whitley*, 514 U.S. 419, 437 (1995).
20 This requirement is automatic in that it is incumbent on the government to make *Brady/Giglio*
21 disclosures “even in the absence of a request by the defense.” *United States v. Blanco*, 392 F.3d
22 382, 387 (9th Cir. 2004).

23 FRCrP 16 applies both to specified types of evidence (like the defendant’s statements) and,
24 as relevant here, to documents and objects that are “material to preparing the defense.” Fed. R.
25 Crim. P. 16(a)(1)(E)(i). This latter requirement is “broader than *Brady*” and *Giglio*. *United States*
26 *v. Muniz-Jaquez*, 718 F.3d 1180, 1183 (9th Cir. 2013). That is because “[i]nformation that is not
27 exculpatory or impeaching may still be relevant to developing a possible defense.” *Id.* The
28 “relevance” or materiality standard in FRCrP just means that the evidence must have “any

tendency” to make a fact more or less likely. *United States v. Doe*, 705 F.3d 1134, 1151 (9th Cir. 2013). As a result, “[e]ven inculpatory evidence may be relevant” because a “defendant who knows that the government has evidence that renders his planned defense useless can alter his trial strategy[or] seek a plea agreement.” *Muniz-Jaquez*, 718 F.3d at 1183. “To obtain discovery under Rule 16, a defendant must make a prima facie showing of materiality. Neither a general description of the information sought nor conclusory allegations of materiality suffice; a defendant must present facts which would tend to show that the Government is in possession of information helpful to the defense.” *United States v. Mandel*, 914 F.2d 1215, 1219 (9th Cir. 1990) (citations omitted).

As noted, Brody’s motion identified thirteen categories of discovery he sought. *See generally* Mot. The government argues, as a general matter, that it has complied with its discovery obligations and, indeed, has exceeded them. *See generally* Opposition to the Mot. (“Oppo.”) [Dkt. No. 52]. When it comes to the specific categories that Brody seeks, the government argues either that (1) it has already disclosed the relevant documents or information; (2) there is no record in its possession, control, or custody that is responsive to the request that exists; or (3) the documents are irrelevant and/or the disclosure is premature.

1. **Dar.sh Script**

The first category of discovery is what Brody describes as records and logs¹ “that the dar.sh script^[2] was run or used and caused damage.” Mot. 4 (capitalization altered). The government has accused Brody of running a “malicious script” called dar.sh to delete information on FRB’s servers. *See, e.g.*, Indictment ¶ 5.

This request is DENIED. The government represents that it has already produced all records that meet this definition and that support this allegation. *See* Oppo. 17. In particular, the

¹ A log is a computer file that records events. *See, e.g.*, Abby Braden, *Log*, Webopedia, <https://www.webopedia.com/definitions/log/>. All of the footnotes in this order are meant solely for context, not to determine any adjudicative fact or to supply a complete technical definition.

² A scripting language is a computer programming language that causes computer programs to run. *See Scripting language*, Merriam-Webster Dictionary (11th ed. 2020). A script is a section of code that executes a task on the computer. *See, e.g.*, *Script*, PCMag Encyclopedia, <https://www.pcmag.com/encyclopedia/term/script>.

government cites (1) a thumb drive it produced that contains FRB logs, (2) logs from Brody's computer that allegedly shows he ran `dar.sh`, and (3) a summary of FRB's internal investigation describing the script. *Id.* In response, Brody does not dispute that these were given to him. *See* Reply ISO Mot. ("Reply") [Dkt. No. 56] 2–3. Instead, he argues that the allegations against him include that he *ran* the script, but this cited evidence shows only that it was *created* or *modified*. *See id.*

This is the only evidence of running the script that the government represents it has; it cannot disclose evidence that does not exist. Brody's argument is really evidentiary or merits-based: he does not believe that this evidence adequately shows that he ran `dar.sh` (as opposed to had possession of it or modified the code), which is an argument for a factfinder. But there is no indication of any withheld evidence.

Still more, this evidence does (at least arguably) support the government's allegation that Brody ran the script, so his argument that there is other evidence that must back up that allegation falters on its own terms. Specifically, one of the three types of evidence that the government cites is Brody's computer logs that, it asserts, record him having *run* `dar.sh`. *See* Oppo. 17. While Brody disputes that the *other two* types of evidence in fact show that, his brief does not dispute that this one does. *See* Reply 2–3.

2. GitHub Firewall Logs

Brody next moves to compel discovery of logs of firewall³ access from GitHub, which presumably helps host FRB's systems. *See* Mot. 5. These logs, says Brody, "show user activity and traffic to the FRB GitHub including which user devices were connected to the FRB GitHub during the period of the alleged intrusion." *Id.* The government alleges that Brody accessed the FRB GitHub and caused damage to it. *See, e.g.,* Indictment ¶¶ 4, 8, 14.

The request is DENIED. The government represents that it has turned over all documents that meet this criterion. *See* Oppo. 17. Specifically, it cites (1) screenshots of Github access logs,

³ A firewall is "[a]n inter-network connection device that restricts data communication traffic between two connected networks." National Institute of Standards and Technology, *Firewall*, Computer Security Resource Center, <https://csrc.nist.gov/glossary/term/firewall#>.

(2) a spreadsheet of the Github firewall logs, and (3) screenshots of the firewall logs. *Id.* At the hearing, based on some ambiguity left from Brody’s reply brief, *see* Reply 3, about whether these records were sufficient, I asked the government to confirm that these records were the only ones it possessed that could qualify. The government confirmed that, to the extent any responsive record exists, it was within these disclosures. Because this is the evidence the government is relying on for that allegation, it is bound to it. Once again, Brody’s issue appears to be better characterized as an argument that the records do not, as a factual matter, adequately support a charge.

3. Taunt Code

The third category seeks multiple types of records united by the common theme of “taunt” code. *See* Mot. 5–6. As alleged, Brody left a few “taunts” in the code that he unleashed on FRB. *See, e.g.,* Indictment ¶ 6. In particular, he is alleged to have used the word “grok,” which the government explains is a misspelling of “grock,” which, in turn, means to understand. *See* Oppo. 1 n.1; Compl. ¶ 18. Brody asks for three types of records related to this: those that include the question, “Do you grok it now?”; those that reference grockit.pem; and any others that support allegations of “code-related taunts.” Mot. 5. Additionally, Brody seeks “all communications” with FRB about these. *Id.*

The request is DENIED. The government represents that it does not have any code stating “Do you grok it now?”; instead it supported that allegation with *witness statements* by individuals who saw that code. Oppo. 17. It turned those over to Brody. *Id.* The government also cites specific produced documents that reference “grockit.pem.” *Id.* 18. The government is unaware of any way in which the catchall category of other “code-related taunts” is different than just these two examples. *Id.* And, to address the communications with FRB, the government produced summaries of witness interviews with FRB employees. *Id.* The government says that it has no other responsive documents. *Id.* 17. Brody’s response is, once again, a merits argument: that these documents do not adequately support the allegations. *See* Reply 4–6. Again, that may be for another day, but it does not mean there is more to disclose.

4. Apke Email References

Alex Apke is a cloud engineer with FRB; it appears that Brody believes that he accessed

the FRB network on March 11 and 12, 2020, made changes, and caused damage. *See* Mot. 6. This exhibit request relates to an email that Apke sent on March 12, 2020. *See* Dkt. No. 51-2 (copy of email exchange). Brody moves to compel the government’s disclosure of several records or items referenced in the email: (1) a particular file; (2) home directories⁴ where “bash history” is storied; (3) Hashicorp Zendesk incident tickets that Apke and another person opened on March 12, 2020; (4) account usage for the services senthil.pem, grockit.pem, and z_lnxadm; (5) certain passwords; and (6) resetting one password. *See* Mot. 6.

The request is DENIED. The government represents that it already has turned over all records related to this request. *See* Oppo. 18. In particular, the government has produced the attachments to the email, *see id.*, which Brody references, *see* Mot. 6. And the government has produced evidence authenticating that those attachments are complete. *See* Oppo. 18. It has, separately, produced all records it has relating to the three services discussed by name above. *See id.* Brody’s reply does not point to any concrete reason to think the government has more files related to these categories. Instead, he asks that the government identify the Bates numbers for all of this production. At the hearing, however, the government represented that the material cited in its brief (that is, on page 18 of the Opposition) was all that it believed was responsive to this request in its possession. On that basis, there is no need for it to produce the Bates numbers.

5. Home Directories and Files of FRB Users

Brody moves to compel disclosure of home directories and files of FRB users on specified services. Mot. 7. His reply accepts the government’s representation that it has no responsive materials. *See* Reply 12. Accordingly, this request is moot.

6. Git Scripts

Brody moves to compel disclosure of (1) git log⁵ and git commit history⁶ for a particular

⁴ A home directory is “[a] storage folder that contains the user’s personal files.” *Home directory*, PCMag Encyclopedia, <https://www.pcmag.com/encyclopedia/term/home-directory>.

⁵ A git log “is a utility tool to review and read a history of everything that happens to a repository.” *Git log*, JavaTPoint, <https://www.javatpoint.com/git-log>.

⁶ A git commit history appears to be a log that overlaps substantially with the git log: it contains a history of the “commits”—that is the, changes—to a file. *See, e.g.,* Anthony Heddings, *How to View Commit History with Git Log*, How-To Geek, <https://www.howtogeek.com/devops/how-to->

script and (2) a list of users who “checked out” that script during that time. Mot. 8. The script at issue is the “Repo.discovery” script that was allegedly used to delete and damage FRB’s systems. *See id.* While the government has disclosed the script itself, says Brody, it has not disclosed the git log, git commit history, and list of users who checked it out. *Id.* The government responds that it has produced all records it has and that any others are in FRB’s possession, not in its possession. Oppo. 19. In particular, the government produced all FRB logs it has, including logs of a script called “hook.destroy” that it alleges Broody ran. *Id.*

Brody’s reply brief maintains that the government’s response is ambiguous. But if anything is unclear it is the provenance of the “Repo.discovery” script. As noted, “hook.destroy” is what the government alleges Brody ran. Brody’s briefing does not explain why he believes “Repo.discovery” is material to the case. He has submitted a sworn declaration discussing many topics, including this one; but the relevant paragraphs never tie “Repo.discovery” to anything the government has alleged. *See* Dkt. No. 51-1 ¶¶ 61–69. It seems, perhaps, Brody seeks this because it was a script used during the regular course of FRB’s business to delete files. *See id.* But that does not mean the government has anything to disclose about it. It appears that FRB might, which Brody may seek through ordinary discovery mechanisms. The request is DENIED.

7. PingFederate Records

Brody’s motion sought records of FRB users (called PingFederate records) that authenticate who those users were. Mot. 8. His reply brief accepts the government’s representation that it has no records that are responsive. Reply. 12. Accordingly, this request is moot.

8. Specified User Records

Brody’s motion sought records of FRB users that fell into four specified categories (CloudTrail, MFA, VPN, Traffic). Mot. 8. His reply brief accepts the government’s representation that it has no records that are responsive. Reply. 12. Accordingly, this request is moot.

view-commit-history-with-git-log/.

9. March 11 Meeting Communications

As noted, Brody met with FRB management on March 11 about the alleged inappropriate content on the thumb drive. Indictment ¶ 2. The government alleges that Brody “was told to bring his company-issued 2018 Apple 15” MacBook Pro laptop to his meeting with FRB Human Resources on March 11, 2020, but he did not.” *Id.* Brody now seeks to compel the government to disclose any written communications or records that directed Brody to bring his laptop to that meeting. Mot. 9.

This request is DENIED. The government represents that it has turned over many documents relevant to the meeting; it cites one document by Bates number. *See* Oppo. 19. Brody responds that there is no *written* record that has been disclosed, which is what it seeks. But the portion of the Indictment on which this request relies does not allege anything different; it just states that Brody “was told” to bring that laptop. Indictment ¶ 2. That statement is relevant because it illustrates why the government has responded to the request as it did.

10. Last Connection by dbrody

Brody moves to compel disclosure of any records concerning the last connection of his account with the username dbrody to FRB’s network. Mot. 9. He seeks this because the government has alleged that FRB terminated Brody’s access on March 12, 2020, and “[t]he malicious activity ended after Brody’s credentials were terminated.” Indictment ¶ 7.

The request is DENIED for today. The government represents it has turned over all records on this issue. Oppo. 19–20. Unlike its other representations like this, however, it does not cite any specific documents. *See id.* Accordingly, it shall identify by Bates number for Brody which documents it is referring to.

11. Chain of Custody of Network Intrusion Records

Brody moves to compel disclosure of the “chain of custody and how records were collected concerning the March 11-12 2020 network intrusion.” Mot. 9. The government replies that this evidence is irrelevant now because whether something has an appropriate chain of custody is to be proved at trial. *See* Oppo. 15–16, 20. And, it contends, “chain of custody” evidence is “largely irrelevant” to network intrusion cases because it is more properly geared

1 toward the chain of custody of physical evidence. *Id.* 16. In his reply brief, Brody argued for the
 2 first time that “[q]uestions have been raised about the integrity” of specific digital evidence.
 3 Reply 8. He cites two examples, the thumb drive and attachments to the Apke email referenced
 4 above, to which alleged alterations or modifications appear to have been made after the evidence
 5 entered the government’s possession. *See id.* 8–9.

6 This request is DENIED. Based on Brody’s new arguments in the reply brief, I asked the
 7 government at the hearing to explain its views on the alleged alterations or modifications. The
 8 only thing that even arguably fits the bill, the government contends, are “placeholders” made
 9 when government attorneys and paralegals transmitted the data to Brody’s counsel. Those
 10 placeholders, moreover, are the same as were created when the government made a second
 11 production of records, further indicating that is all they are. At the hearing, Brody’s counsel
 12 offered no specific argument that would contradict this. And in any event, Brody’s counsel can
 13 obtain original files from FRB and the government will ultimately have to authenticate the data,
 14 so special disclosure of a chain-of-custody declaration is not warranted at this point.

15 **12. Preservation Requests**

16 Brody moves to compel disclosure of the government’s requests to preserve records or data
 17 to FRB, internet service providers (“ISPs”), other wire/electronic services, and other companies.
 18 Mot. 10. The government again argues that this evidence is irrelevant. *See* Oppo. 15–16, 20. The
 19 request is DENIED for today. At this point, it appears likely that the documents are work product
 20 that cannot be disclosed now under Rule 16. *United States v. Armstrong*, 517 U.S. 456, 463
 21 (1996) (“Under Rule 16(a)(1)(C), a defendant may examine documents material to his defense,
 22 but, under Rule 16(a)(2), he may not examine government work product in connection with his
 23 case.”).⁷ And Brody has not shown they are exculpatory or impeaching at this stage to warrant
 24 production under *Brady* or *Giglio*. Brody is free to subpoena FRB, the ISPs, and related entities
 25 for information. If, after discovery is otherwise completed, Brody can make a more particularized

26
 27 ⁷ The case that Brody contends is on-point about this issue did not consider the work-product
 28 doctrine. *See United States v. W.R. Grace*, 233 F.R.D. 586 (D. Mont. 2005). It also concerned the
 materially different situation of documents related to preserving environmental sampling that the
 government had placed on its exhibit list in a Clean Air Act case. *See id.* at 587–89.

showing of need based in part on deficient responses to his good-faith attempts to conduct full discovery, he may raise the issue again provided he can make an argument about why the work-product doctrine does not apply.

13. Network Diagrams

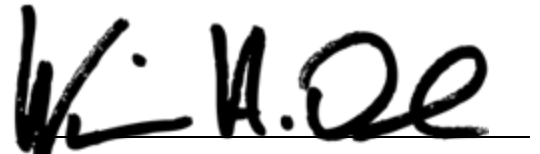
Brody moves to compel disclosure of the “diagram” of FRB’s network. Mot. 10. The government represents, however, that it turned over that diagram on May 27, 2022, after the parties stipulated to their protective order (and after the motion was filed). Oppo. 20. In his reply, Brody argues that this diagram includes a reference to a *former* diagram that was not produced. If the government has this former diagram in its possession, it has given no reason for not producing it. But it appears it does not. If it has the diagram, it is ordered to produce it; if it does not, there is no further dispute between the parties and the request is denied on that understanding.

CONCLUSION

The motion to compel discovery is DENIED.

IT IS SO ORDERED.

Dated: July 13, 2022


 William H. Orrick
 United States District Judge